**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

The physical security measures that can be put in place to protect a network are:

* Storing in a locked room
* Installing alarms to warn off intruders

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

An organisation could use a passwords that are at least eight digits long, include characters that are non-alphabetical, the organisation should not make the passwords easy to guess and should change them regularly.

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters the incoming information coming through the internet, any packet of data that is flagged as unwanted is not allowed through to the organisations internal network.

1. What are the main purposes of firewalls and how are these purposes achieved?

The main purpose of firewalls is to prevent infiltration from the outside; the firewall achieves this as it has no holes.

1. Why do firewalls use 2 separate NICs?

Firewalls use two separate NICs because one is connected to the internal network and the other is connected to the outside. The data is then filtered from the outside NIC through to the computer and what is found to be safe is passed through to the inner NIC.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware is malicious software (including spyware, adware, Trojan horses, worms and viruses), to protect against malware network administrators will have the workstations run virus protection software, the antivirus software is updated as soon as possible and automatically through the network, a firewall is also put in place to block malware from sending personal information across the internet, administrators will also use anti-adware programs on workstations.

**Encryption**

1. What is encryption?

Encryption is the process of translating data into a secret code that can only be read by authorised users. To read the data the user must have access to the secret key to decrypt the data.

1. Describe the nature of WPA or WPA2.

WPA or WPA2, Wi-Fi protected access is a security protocol for use on a wireless LAN. It provides the LAN with security by encrypting data to be sent over the radio waves, so it is protected during transmission, it was designed to give wireless networks the same security as wired networks.

1. What is encrypted data known as?

Encrypted data is known as ciphertext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

The secure protocol that allows financial transactions is hypertext transfer protocol security or https, it ensures a secure connection is established and maintained between the client’s web browser and the web server. Transactions are encrypted and authenticated as they travel across the internet.

1. What is digital identification certificate technology based on?

The digital identification certificate technology is based on a trusted certificate authority.

1. Describe the nature of Secure sockets layer (SSL) protocol.

The Secure sockets layer is a cryptographic protocol that provides a secure connection on the internet. When a client’s web browser points to a secured domain the SSL authenticates the website and the client, an encryption method is then established with a unique session key and secure transaction begins.

**Physical design of networks**

1. What is the role of a network diagram?

The role of a network diagram is to show the physical devices and communication lines present in a network, this makes it easier for technical support people to find and identify equipment in the network. In a network diagram straight lines are used to represent cables and icons are used for the devices.

Darcie Anderson